Sdshelter 2.0

エスディシェルター ver.2.0 管理者ツール

取扱説明書

（通常版／アカデミック版共通）

第 4 版

ed-contrive®
イーディーコントライブ株式会社

目次

はじめに

Sdshelter 2.0 管理者ツールでできること----------4
同梱品----------7
動作環境----------7
Sdshelter 2.0 管理者ツールのインストール----------8

ポリシー設定ツールの操作

ポリシー設定ツールの起動----------9
パスワード桁数の設定----------9
パスワード使用文字種の設定----------10
パスワードの必須使用文字種の設定----------10
パスワードの有効期間の設定----------11
24 時間内のパスワード変更可能回数の設定----------11
パスワード履歴によるパスワード制限の設定----------12
パスワード認証失敗制限回数の設定----------12
パスワード忘れ／ロック時の救済機能設定----------13
マスターパスワードの設定----------13
使用可能期限設定----------14
ウィルス対策ソフトウェアのチェック機能の設定----------14
ドライブサイズの設定----------15
ボリュームラベルの設定----------15
追加ファイルの設定----------16
Autorun.inf ファイル削除設定----------16
アクセス許可プロセス（オフィス外用）の設定－①----------17
アクセス許可プロセス（オフィス外用）の設定－②----------18
流出防止オプション（オフィス外用）の設定----------18
ログ取得機能の設定----------19
ログファイル自動削除の設定----------20
ウィンドウログの設定----------21
プロセスログの設定----------22
ファイルアクセスログの設定－①----------23
ファイルアクセスログの設定－②----------24
キーボードログの設定----------25
インターネットアドレスログの設定----------26
初期化ツール ID の設定----------27

初期化ツール／ドライバインストーラーの保存----------27
設定内容の確認／設定の保存----------28

初期化ツールの使用----------29

使用可能期限の設定----------30

ロック解除・パスワード強制変更----------31

ソフトウェア環境毎の主なドライバ機能の比較----------33

ソフトウェア使用許諾書----------34

◎Microsoft、Windows、Windows 2000/XP/Vista/ 7 は、Microsoft Corporation の米国及びその他の国における登録商標または商標です。
◎その他、記載されている会社名、製品名は各社の登録商標または商標です。

はじめに

Sdshelter 2.0 管理者ツールでできること

Sdshelter 2.0 管理者ツールは、セキュリティ USB メモリ「Sdshelter 2.0」に対して、パスワードの桁数・パスワード忘れ／ロック時の救済機能・使用可能期限機能・ウィルス対策ソフトウェアのチェック機能・オフィス外 PC でのネットワークアクセス／印刷の禁止等、セキュリティポリシーの設定を行なえるシステム管理者用ソフトウェアです。

Sdshelter 2.0 管理者ツールは以下のツールで構成されています。

- ポリシー設定ツール
- 期限設定ツール
- レスキューツール

上記のツールはそれぞれ独立してインストールが可能であるため、ツール毎に使用者（インストール先 PC）を変更して、お客様の運用に合わせてご利用いただけます。

ポリシー設定ツール

Sdshelter 2.0 のポリシーを設定し、Sdshelter 2.0 へ反映させるための初期化ツールと、オフィス内 PC で Sdshelter 2.0 を利用可能にするためのオフィス内ドライバのインストーラーを作成するツールです。また、ポリシーの設定によりオフィス外 PC で Sdshelter 2.0 を利用可能にするためのオフィス外ドライバのインストーラーも作成することが可能です。ポリシー設定ツールの使用方法は P. 9～をご参照ください。

ポリシー設定ツール　　初期化ツール　　オフィス内ドライバのインストーラー　　ポリシーの設定によりオフィス外ドライバのインストーラー

＊ ポリシーの設定により、オフィス外ドライバのインストールが必要の無い［インストールレス機能（管理者権限時にオフィス外動作）］を利用することも可能です。設定方法等は、P. 18 をご参照ください。

初期化ツール

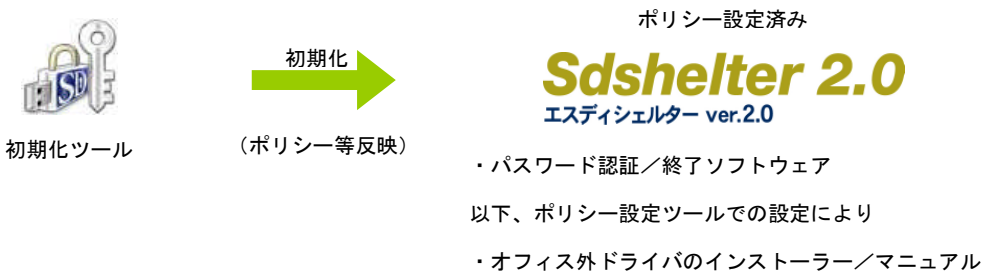
ポリシー設定ツールで作成する、Sdshelter 2.0 にポリシーを反映するためのツールです。インストール無しで実行可能ですので、初期化ツールを配布し、配布先でポリシーを反映した Sdshelter 2.0 を作成する等の運用が可能です。

その他、初期化の際に Sdshelter 2.0 内に作成されるソフトウェア等

- Sdshelter 2.0 へのパスワード認証用（SDS2.exe）
- 機能の停止からアンマウント迄を行う Sdshelter 2.0 の終了用（SDS2Stop.exe）

以下、ポリシー設定ツールでの設定により

- オフィス外ドライバのインストーラー（SDS2Driver_Out.exe）
- オフィス外ドライバのインストールマニュアル（SDS2Driver_Out_Installmanual.pdf）



また、個別にポリシー設定が行われた Sdshelter 2.0 では、予め設定した初期化ツール ID が一致しない限り、別の初期化ツール ID を持つ初期化ツールでの再設定ができませんので無断で設定が変更される心配がありません。初期化ツールの使用方法は P. 29 をご参照ください。

オフィス内ドライバのインストーラー（SDS2Driver_In. exe）

ポリシー設定ツールで作成する、オフィス内 PC で Sdshelter 2. 0 を利用可能にするオフィス内ドライバです。また、各種ログを取得し Sdshelter 2. 0 内に記録させることも可能です。インストーラーでのオフィス内ドライバのインストール方法等は、別紙のオフィス内ドライバ取扱説明書（PDF）をご参照ください。

オフィス外ドライバのインストーラー（SDS2Driver_Out. exe）

オフィス外 PC で Sdshelter 2. 0 を利用可能にし、コピーガード機能を備えたオフィス外ドライバです。また、各種ログを取得し Sdshelter 2. 0 内に記録させることも可能です。インストーラーの作成方法は、P. 16 の追加ファイルの設定をご参照ください。また、インストーラーでのオフィス外ドライバのインストール方法等は、別紙のオフィス外ドライバ取扱説明書（PDF）をご参照ください。

＊ ポリシーの設定により、オフィス外ドライバのインストールが必要の無い［インストールレス機能（管理者権限時にオフィス外動作）］を利用することも可能です。設定方法等は、P. 18 をご参照ください。

期限設定ツール

期限設定機能が有効に設定されている Sdshelter 2. 0 に対して使用可能期限を設定／再設定するツールです。期限設定ツールを使用した使用可能期限設定方法はP. 30 をご参照ください。

レスキューツール

パスワード忘れ／ロック時の救済機能設定が有効な Sdshelter 2. 0 に対して、パスワードの強制再設定、及びロック解除を行うために使用するツールです。レスキューツールを使用したパスワード忘れ／ロック時の救済方法はP. 31～をご参照ください。

同梱品

Sdshelter 2.0 管理者ツールには次のものが同梱されています。開封後、ご確認ください。

① CD-ROM　1 枚　（CD-ROM 内のフォルダ構成は以下の通りです）

```
［ Sdshelter 2.0 管理者ツール ］
　└［ installer ］
　　├ Setup_SDS2Policy. exe
　　├ Setup_SDS2Period. exe
　　└ Setup_SDS2Rescue. exe

［ Sdshelter 2.0 管理者ツール ］
　└［ manual ］
　　├ SDS2AdminTool_manual. pdf
　　├ SDS2Driver_In_Installmanual. pdf
　　└ SDS2Driver_Out_Installmanual. pdf
```

② Sdshelter 2.0 クイックガイド　1 枚

＊ 同梱品が足りないときや破損しているときは、当社もしくは販売店にご連絡ください。

動作環境

Sdshelter 2.0 管理者ツール（ポリシー設定ツール、期限設定ツール、レスキューツール）

OS	Microsoft Windows 2000 Professional SP4 日本語版 Microsoft Windows XP Professional SP2 以降 日本語版 Microsoft Windows XP Home Edition SP2 以降 日本語版 Microsoft Windows Vista ～SP2 日本語版 Microsoft Windows 7 日本語版 ＊ 64 ビット OS には、未対応です ＊［インストールレス機能（管理者権限時にオフィス外動作)］は、 Microsoft Windows 2000 ではご利用いただけません
CPU	Intel Pentium Ⅲ 1GHz 以上
メモリ	256MB 以上　＊ Vista 、7 に関しては 512MB 以上
その他	CD-ROM を再生できる倍速以上のドライブが必要です。

ポリシー設定ツールから作成される初期化ツール

OS	Microsoft Windows 2000 Professional SP4 日本語版 Microsoft Windows XP Professional SP2 以降 日本語版 Microsoft Windows XP Home Edition SP2 以降 日本語版 Microsoft Windows Vista ～SP2 日本語版 Microsoft Windows 7 日本語版 ＊ 64 ビット OS には、未対応です
CPU	Intel Pentium Ⅲ 1GHz 以上
メモリ	256MB 以上　＊Vista 、7 に関しては 512MB 以上
その他	USB ポート　USB2.0 が必要です。 管理者権限を持つアカウントで実行する必要があります。

Sdshelter 2.0 管理者ツールのインストール

Sdshelter 2.0 管理者ツールの下記各ツールは、お客様での運用にあわせ、ご利用される PC のアカウント毎にインストールが必要です。アンインストールするには、インストールを行ったツール／アカウント毎に操作が必要となります。

各ツールのインストーラーのファイル名は以下の通りです。

・ポリシー設定ツール：Setup_SDS2Policy. exe
・期限設定ツール　　：Setup_SDS2Period. exe
・レスキューツール　：Setup_SDS2Rescue. exe

＜インストール＞

コンピュータの CD-ROM ドライブに Sdshelter 2.0 管理者ツールの CD を挿入します。CD-ROM ドライブのインストーラープログラムをダブルクリックします。インストーラーに従って操作してください。

＜アンインストール＞

［スタート］→［コントロールパネル］→［プログラムのアンインストール］（Windows XP の場合は［プログラムの追加と削除］、Windows 2000 の場合は［アプリケーションの追加と削除］）をクリックします。アンインストールする対象のツールを選択し、アンインストールを行ってください。

各ツールは下記の通り表示されます。

・ポリシー設定ツール：Sdshelter 2.0 ポリシー設定ツール
・期限設定ツール　　：Sdshelter 2.0 期限設定ツール
・レスキューツール　：Sdshelter 2.0 レスキューツール

ポリシー設定ツールの操作

ポリシー設定ツールの起動

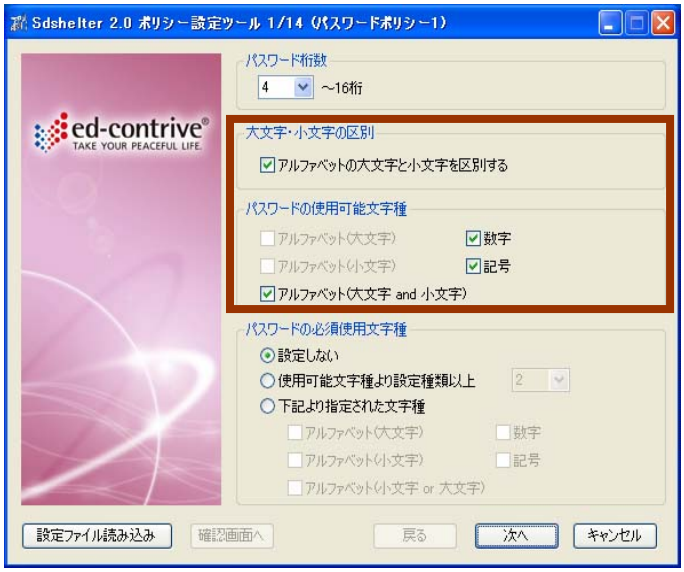
［スタート］→［(すべての)プログラム］→［ED-CONTRIVE］→［Sdshelter 2.0］→［Sdshelter 2.0 ポリシー設定ツール］を選択します。ポリシー設定ツールが起動します。

パスワード桁数の設定

パスワードの最小桁数を 1～16 桁の間で設定可能です。(デフォルトは 4 桁です。)

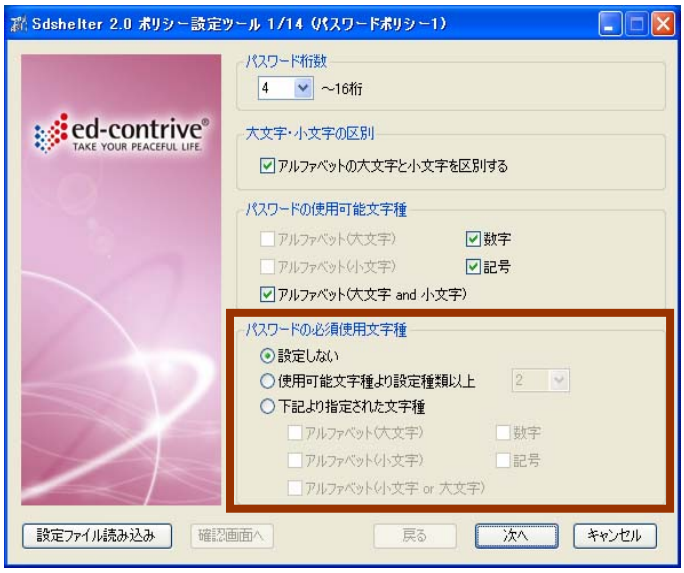
パスワード使用文字種の設定

パスワードに使用する文字種が設定可能です。使用したい文字種を選択してください。(パスワードに使用する文字種は全て半角になります。)



パスワードの必須使用文字種の設定

パスワードの入力必須文字種として設定したい文字種を選択してください。



パスワードポリシー1 の設定が完了したら、[次へ] をクリックします。

パスワードの有効期間の設定

パスワードの有効期間を設定する場合は［パスワードの有効期間日数を設定する］をチェックし、10 日～180 日の範囲で選択してください。

24 時間内のパスワード変更可能回数の設定

パスワードを 24 時間の間に変更可能な回数を設定します。初期パスワードの設定も 1 回としてカウントされます。

尚、パスワード設定時からパソコンの時間を戻す操作（24 時間以上）を実施した場合は、回数によらずパスワード変更ダイアログが表示されます。

パスワード履歴によるパスワード制限の設定

過去に使用したことのあるパスワードを設定できないようにします。（現在使用しているパスワードを 1 回目としてカウントします）
履歴として 1～10 回目までのパスワードの禁止設定が可能です。

パスワードポリシー2 の設定が完了したら、［次へ］をクリックします。

パスワード認証失敗制限回数の設定

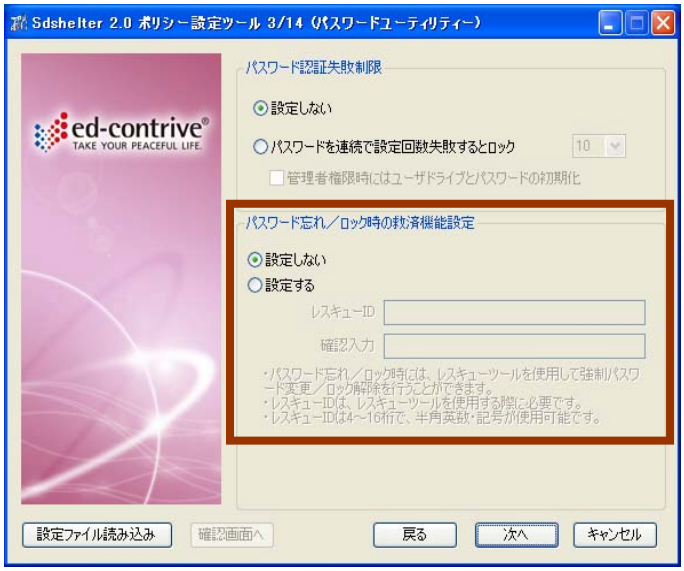
パスワード認証連続失敗制限回数の設定が可能です。設定した回数分パスワード認証に連続で失敗した場合は、Sdshelter 2.0 のユーザードライブはロックされ、正しいパスワードを入力しても使用できない状態となります。

［管理者権限時にはユーザードライブとパスワードの初期化］をチェックすると、管理者権限でご利用の際に、設定回数分パスワード認証に連続で失敗するとロックではなく、ユーザードライブのデータとパスワードを初期化します。

注意	＊［管理者権限時にはユーザードライブとパスワードの初期化］の実行後、パスワードポリシー等は引き継がれますが、ユーザードライブの追加ファイルやログファイルについては、復旧致しません。

パスワード忘れ／ロック時の救済機能設定

パスワードを忘れた場合や、パスワード認証連続失敗制限の設定回数分連続で失敗してロックされた場合の救済機能です。
本機能を有効にすると、本操作で設定するレスキューID とレスキューツールを使用してロック解除／パスワード強制変更を行うことができるようになります。
パスワード忘れ／ロック時の救済方法の操作についてはP. 31～をご参照ください。



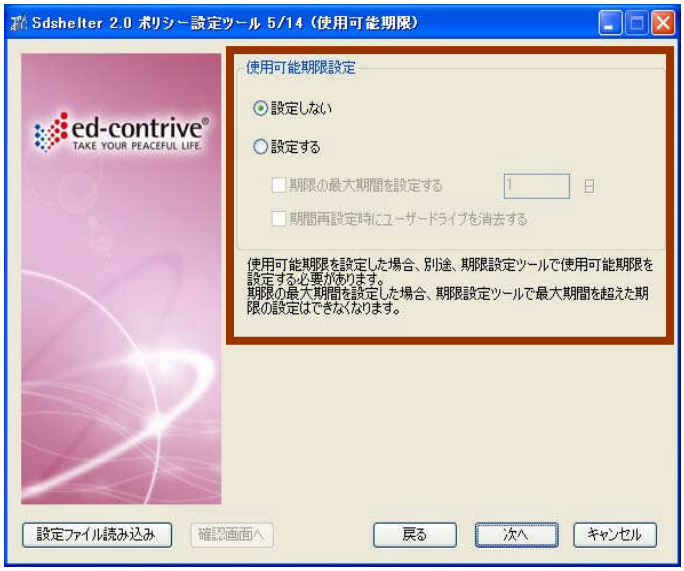
パスワードユーティリティーの設定が完了したら、［次へ］をクリックします。

マスターパスワードの設定

マスターパスワードを設定していると、パスワードを忘れた際にも、マスターパスワードを使用してユーザードライブを開くことが可能です。
同じ初期化ツールで設定した Sdshelter 2.0 全てに対して、マスターパスワードが有効になりますので、マスターパスワードの設定、取り扱いについてはご注意ください。

マスターパスワードの設定が完了したら、［次へ］をクリックします。

使用可能期限設定



Sdshelter 2.0 の使用期限を設定することが可能です。期限の設定・再設定は期限設定ツールを使用します。

期限の最大期間は、期限設定ツールによる期限設定時から数えて 1～365 日の間で設定可能です。［期限再設定時にユーザードライブを消去する］をチェックしていると、期限の再設定時に Sdshelter 2.0 のユーザードライブに保存されているデータが削除されます。

使用可能期限の設定方法については、P. 30 を参照ください。

注意	＊ 使用可能期限設定を有効にした場合は、期限設定ツールによる期限の設定を行わないと使用できません。本機能を有効にした Sdshelter 2.0 のご利用開始前に期限設定ツールによる設定を行ってください。

使用可能期限の設定が完了したら、［次へ］をクリックします。

ウィルス対策ソフトウェアのチェック機能の設定

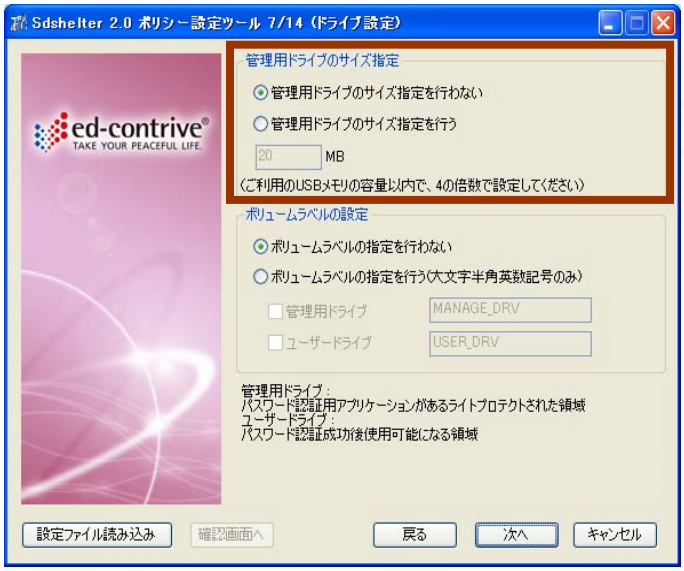
Sdshelter 2.0 を使用する PC でウィルス対策ソフトウェアが有効になっているか、最新状態であるかをチェックし、チェックした結果による動作を設定することができます。

注意	＊ ウィルス対策ソフトウェアが有効になっているか、最新状態であるかは、OS の WMI（Windows Management Instrumentation）という情報収集機能を利用してチェックします。 ＊ チェック結果はウィルス対策ソフトウェアの仕様に依存します。ウィルス対策ソフトウェア及びバージョンによっては、本機能が有効に働かない場合があります。 ＊Windows XP SP2 より古い OS のバージョンにおいては、ウィルス対策ソフトウェアがチェックできない OS として動作します。

ウィルス対策ソフトウェアのチェック機能の設定が完了したら、［次へ］をクリックします。

ドライブサイズの設定

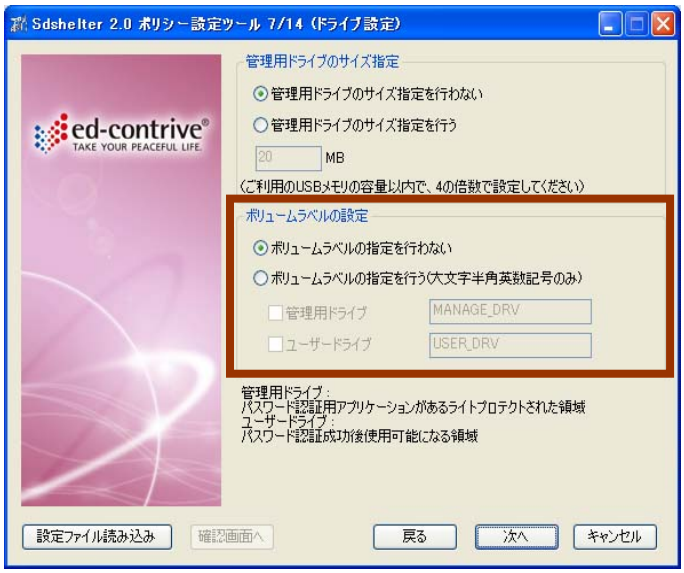
管理用ドライブのサイズを 20MB 以上で設定することが可能です。
管理用ドライブに割り当てた残りがユーザードライブに割り当てられます。
USB メモリの容量以上に設定した場合は、初期化ツールによるポリシー設定ができないためご注意ください。



ボリュームラベルの設定

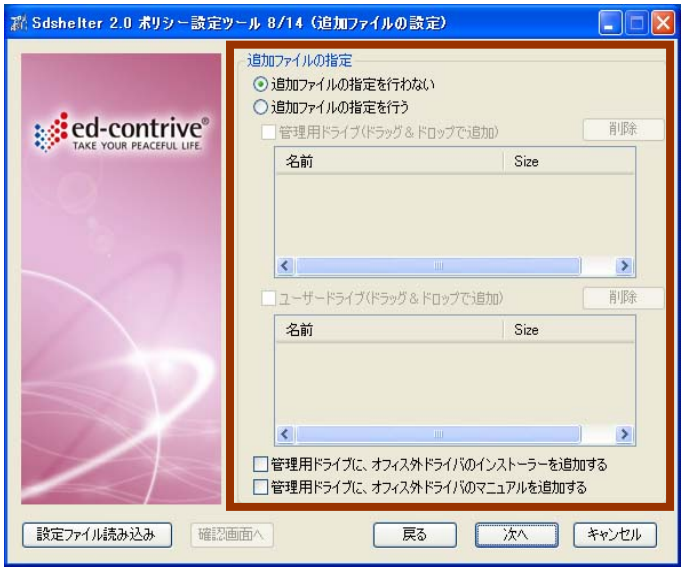
ボリュームラベルをデフォルトから変更することが可能です。
デフォルト設定は以下の通りです。

管理用ドライブ：MANAGE_DRV
ユーザードライブ：USER_DRV



ドライブ設定が完了したら、［次へ］をクリックします。

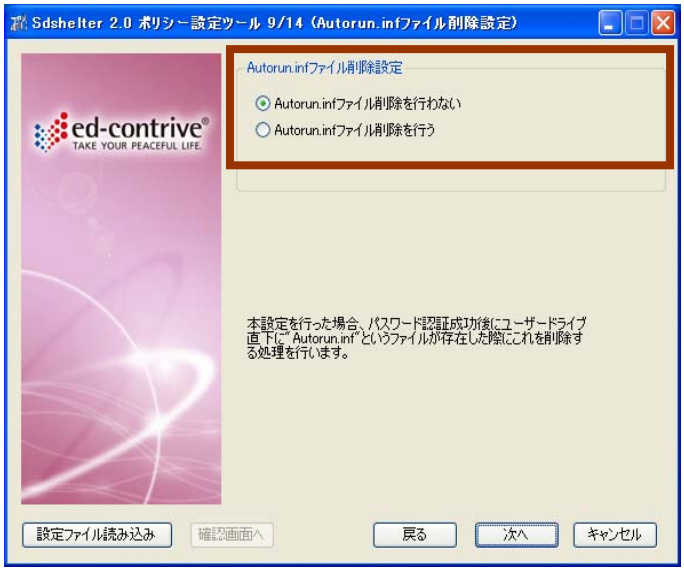
追加ファイルの設定



予め、任意のファイルを Sdshelter 2.0 に追加しておくことが可能です。追加先ドライブをチェック後、ファイルをドラッグ＆ドロップしてください。
また、[管理用ドライブに、オフィス外ドライバのインストーラーを追加する] や [管理用ドライブに、オフィス外ドライバのマニュアルを追加する] が有効の場合、それぞれ当該ファイルを管理用ドライブに追加します。オフィス外ドライバのインストーラーに関しては、管理用ドライブに追加しない場合（無効の場合）、後ほど出力する初期化ツールと共に出力されます。
尚、管理用ドライブのファイルはユーザーでの削除はできません。但し、Sdshelter 2.0 外へのコピーや保存は可能なドライブですので、ご注意ください。
追加ファイルの容量に伴い、初期化ツールの容量も増加します。

追加ファイルの設定が完了したら、[次へ] をクリックします。

Autorun.inf ファイル削除設定



本機能を設定した場合、パスワード認証成功後、ユーザードライブ直下に“Autorun.inf”というファイルが存在した際は、これを削除する処理を行います。
Autorun.inf は指定のプログラムを自動実行するための設定ファイルです。予期せぬ悪意を持ったプログラムの実行を防ぐ手段の一つとして有効です。

Autorun.inf ファイル削除設定が完了したら、[次へ] をクリックします。

アクセス許可プロセス（オフィス外用）の設定－①

オフィス外として Sdshelter 2.0 を使用する場合に適用される各設定です。ユーザードライブにアクセスを、行うことができるプロセス*1 を指定します。プロセスを指定することで、アクセスを拒否したいソフトウェア等からの進入を遮断することが可能になります。また、ユーザードライブ内のファイルは、アクセスを許可されたプロセスのファイルだけが、起動することができます。

指定が無い場合は、[パスワード認証時に、自動で許可プロセスを追加する]（P. 18 参照）が有効になります。デフォルトでは、主に以下のプロセスを指定しています。*2

explorer. exe：エクスプローラー /winword. exe：ワード /excel. exe：エクセル
powerpnt. exe：パワーポイント /msaccess. exe：アクセス /notepad. exe：メモ帳
wordpad. exe：ワードパッド /mspaint. exe：ペイント /acrord32. exe：アドビリーダー
taro15. exe ～ taro18. exe：一太郎 2005 ～ 2008
hanako15. exe ～ hanako18. exe：花子 2005 ～ 2008 /sanshiro. exe：三四郎

*1 OS からメモリ領域などの割り当てを受けて処理を実行しているプログラム。
*2 一部情報漏洩に関わる部分の機能については、制限をもうけております。

［追加］ボタン

［追加］ボタンをクリックすると、プロセスの追加画面が表示されます。入力エリアに追加したいプロセス名を直接入力するか［参照］ボタンをクリックして、プロセス名を選択してください。

［編集］ボタン

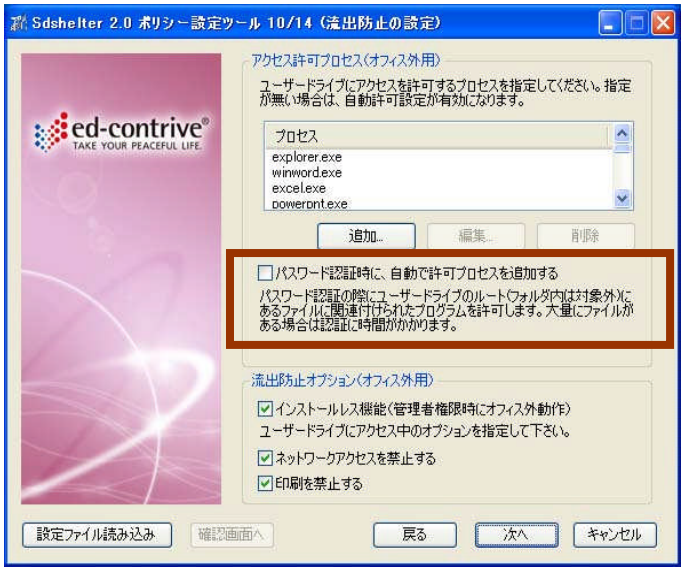
リストに表示されているプロセスを選択後［編集］ボタンをクリックすると、プロセスの編集画面が表示されます。入力エリアに表示されている選択プロセス名を直接編集するか［参照］ボタンをクリックして、プロセス名を選択してください。

［削除］ボタン

リストに表示されているプロセスを選択後［削除］ボタンをクリックすると、選択プロセスはリストから削除されます。

アクセス許可プロセス（オフィス外用）の設定－②

＜［パスワード認証時に、自動で許可プロセスを追加する］チェックボックス＞



本機能を有効にすれば、パスワード認証の際に、ユーザードライブのルートにあるファイルに、関連付けられたプログラム（プロセス）を自動で許可します。

フォルダ内は、対象外です。

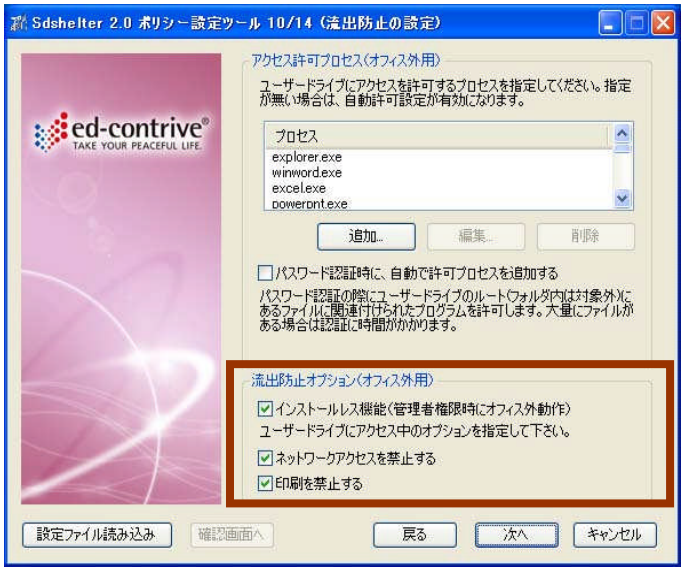
大量にファイルがある場合は認証に時間がかかる可能性があります。

認証の際に、ルートに存在しなかったプログラム（プロセス）のファイルを、認証後にルートへ追加した場合は、次回認証（再認証）時に許可されます。

本機能が有効でも、指定プロセス分はアクセス許可プロセスとして有効です。

デフォルトの指定プロセス以外は、情報漏洩リスクが高くなり、動作しないソフトウェアも発生することがあります。

流出防止オプション（オフィス外用）の設定



オフィス外として Sdshelter 2.0 を使用する場合に適用される各設定です。［インストールレス機能］を有効にすることで、ドライバとポリシー設定ツールがインストールされていない管理者権限を持つアカウント時にはオフィス外機能として、Sdshelter 2.0 を動作させることができます（Windows 2000 は対象外）。当機能に関する補足は、P. 33 をご参照ください。

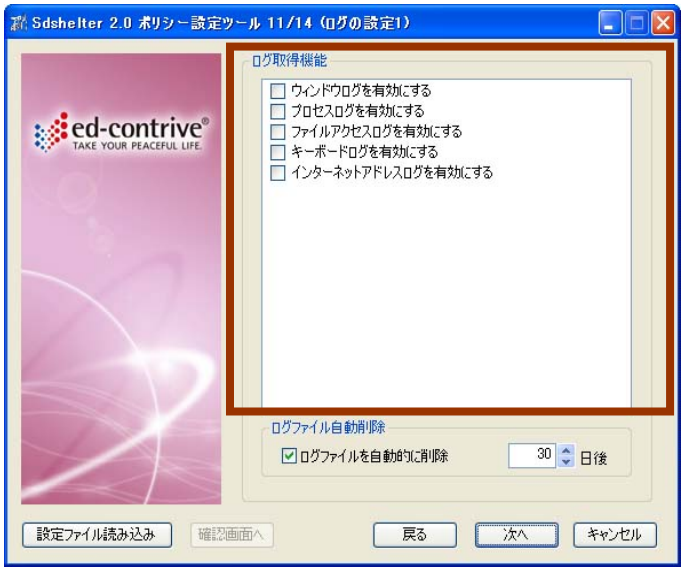
ユーザードライブが有効な間は、ネットワーク又は印刷を禁止する設定が無効の場合、情報漏洩のリスクが高くなります。

流出防止の設定が完了したら、［次へ］をクリックします。

ログ取得機能の設定

記録したいログの種類をリストより、選択してください。
全て未選択の場合は、ログの取得は行いません。

デフォルト設定は全て未選択です。



ユーザードライブが有効な間は、有効設定のログを取得して、ログファイルに蓄積します。

ログファイルは、Sdshelter 2.0 ユーザードライブの Log フォルダ（ログ取得が有効な場合に自動作成）内に、日付単位に複数作成されます。例）090901.log や 090902.log 等

ポリシー設定ツールがインストールされているアカウントでのみ、ログファイル内容の閲覧が可能になります。

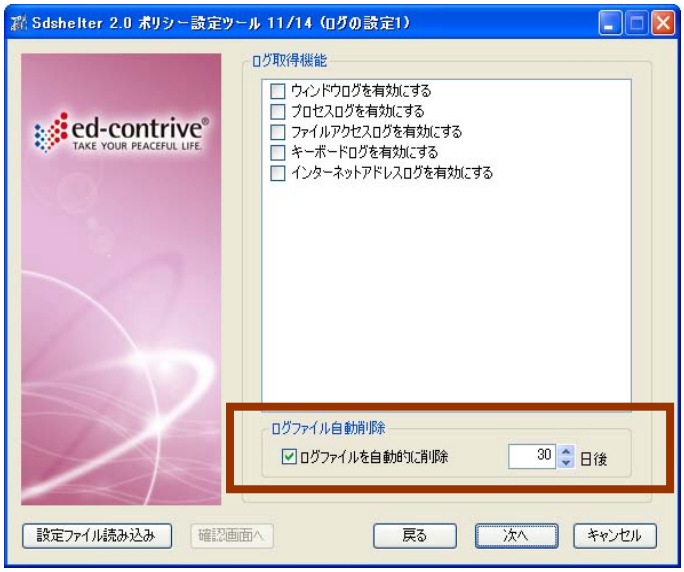
ログの取得は、オフィス内ドライバ又はオフィス外ドライバがインストールされている PC か［インストールレス機能（管理者権限時にオフィス外動作）］として利用する管理者権限を持つアカウント環境下でのみ可能です。

ログファイルの表示内容
例）
09/09/01 16:16:33, プロセス, 「Excel.exe」が起動しました
09/09/01 16:16:33, ファイルアクセス, 「Excel.exe」が「C:¥ed.xls」にアクセスしました
09/09/01 16:16:33, ウィンドウ, 「Microsoft Excel - ed.xls」が開きました
09/09/01 16:16:46, キーボード, 「S」が押されました
09/09/01 16:17:32, インターネットアドレス, 「http://www.ed-contrive.co.jp/」-「イーディーコントライブ」にアクセスしました

ログファイル自動削除の設定

ログファイルを自動的に削除する場合は選択し、日付単位に複数作成される各ログファイルを作成日より何日後に削除するか設定してください。
ユーザーはログファイルを削除できないため、設定することをおすすめ致します。

デフォルト設定は 30 日後自動的に削除するです。



ログの設定 1 が完了したら、[次へ] をクリックします。

ウィンドウログの設定

ログ取得機能の設定で、ウィンドウログを有効にした場合に、設定が可能になります。
ウィンドウログとして残したい項目を選択してください。
ログに残したくないウィンドウタイトルは、除外リストに追加してください。

［ウィンドウが開いた］チェックボックス
開いたウィンドウのウィンドウタイトルを記録します。

［ウィンドウが切り替えられた］チェックボックス
ウィンドウが切り替えられて、アクティブになったウィンドウタイトルを記録します。

除外［追加］ボタン *1
［追加］ボタンをクリックすると、除外ウィンドウタイトルの追加画面が表示されます。
入力エリアに追加したいウィンドウタイトル名を直接入力してください。

除外［編集］ボタン *1
リストに表示されている除外ウィンドウタイトルを選択後［編集］ボタンをクリックすると、除外ウィンドウタイトルの編集画面が表示されます。入力エリアに表示されている選択除外ウィンドウタイトル名を直接編集してください。

除外［削除］ボタン
リストに表示されている除外ウィンドウタイトルを選択後［削除］ボタンをクリックすると、選択除外ウィンドウタイトルはリストから削除されます。

*1 例）Microsoft Excel － ed. xls ：左記に一致するウィンドウタイトルを除外します。

ログの設定２が完了したら、［次へ］をクリックします。

プロセスログの設定

ログ取得機能の設定で、プロセスログを有効にした場合に、設定が可能になります。
プロセスログとして残したい項目を選択してください。
ログに残したくないプロセス*1 は、除外リストに追加してください。

*1 OS からメモリ領域などの割り当てを受けて処理を実行しているプログラム。例）excel. exe

［すでに起動中のプロセス］チェックボックス
ユーザードライブが有効になった時、すでに起動中のプロセスを記録します。

［プロセスの起動］・「プロセスの終了」チェックボックス
それぞれ、プロセスの起動及び終了を記録します。

除外［追加］ボタン
［追加］ボタンをクリックすると、除外プロセスの追加画面が表示されます。入力エリアに追加したいプロセス名を直接入力するか［参照］ボタンをクリックして、プロセス名を選択してください。

除外［編集］ボタン
リストに表示されている除外プロセスを選択後［編集］ボタンをクリックすると、除外プロセスの編集画面が表示されます。入力エリアに表示されている選択除外プロセス名を直接編集するか［参照］ボタンをクリックして、プロセス名を選択してください。

除外［削除］ボタン
リストに表示されている除外プロセスを選択後［削除］ボタンをクリックすると、選択除外プロセスはリストから削除されます。

ログの設定３が完了したら、［次へ］をクリックします。

ファイルアクセスログの設定－①

ログ取得機能の設定で、ファイルアクセスログを有効にした場合に、設定が可能になります。
ファイルアクセスログとして残したいフォルダ又はドライブを追加してください。
特定のプロセスや OS からアクセスされる、指定のフォルダ又はドライブ以下のファイル又はフォルダへのファイルアクセスログを残したくない場合は除外リストに追加してください。

SecretDrive = ユーザードライブ

フォルダ・ドライブ［追加］ボタン（ドライブ全体を指定するとログが大量になります）
［追加］ボタンをクリックすると、フォルダ・ドライブの追加画面が表示されます。(P. 24)

フォルダ・ドライブ［編集］ボタン（ドライブ全体を指定するとログが大量になります）
リストに表示されているフォルダ・ドライブを選択後［編集］ボタンをクリックすると、フォルダ・ドライブの編集画面が表示されます。(P. 24)

フォルダ・ドライブ［削除］ボタン（全てを削除した場合は当該ログ全てを取得します）
リストに表示されているフォルダ・ドライブを選択後［削除］ボタンをクリックすると、選択フォルダ・ドライブはリストから削除されます。

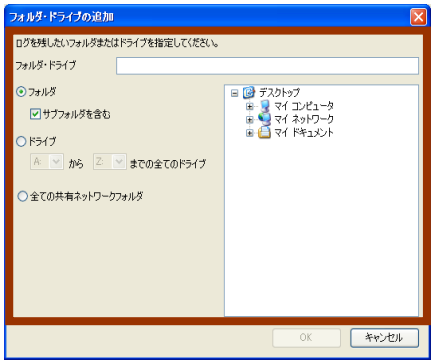
除外［追加］ボタン
［追加］ボタンをクリックすると、除外プロセスの追加画面が表示されます。(P. 24)

除外［編集］ボタン
リストに表示されている除外プロセス/ファイル・フォルダを選択後［編集］ボタンをクリックすると、除外プロセスの編集画面が表示されます。(P. 24)

除外［削除］ボタン（デフォルト設定を削除するとログが大量になります）
リストに表示されている除外プロセス/ファイル・フォルダを選択後［削除］ボタンをクリックすると、選択除外プロセス/ファイル・フォルダはリストから削除されます。

ファイルアクセスログの設定－②

＜［フォルダ・ドライブの追加編集］画面＞



［フォルダ・ドライブ］入力エリア *1

左側の［フォルダ］ラジオボタンを選択後、右側のツリー上で選択するか、左側の［ドライブ］又は［全ての共有ネットワークフォルダ］ラジオボタンを選択するとフォルダ又はドライブが入力エリアに表示されます。直接入力も可能で、ファイル名の指定も行えます。

［フォルダ］ラジオボタン

選択することで、右側のツリー上でフォルダ・ドライブの選択が行えます。

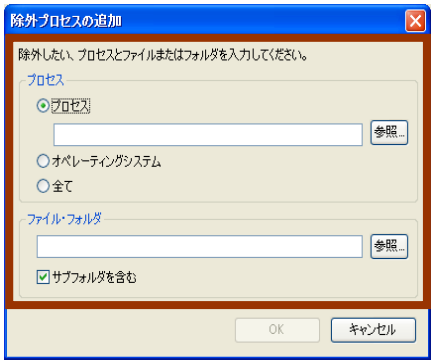
［ドライブ］ラジオボタン

選択することで、ドライブの範囲選択が行えます。

［全ての共有ネットワークフォルダ］ラジオボタン

選択することで、全ての共有ネットワークフォルダを表す文字 ¥¥ が表示されます。

＜［除外プロセスの追加編集］画面＞



［プロセス］ラジオボタン

指定フォルダ・ドライブ以下への、どのプロセスからのアクセスログを除外したいか、直接入力か［参照］ボタンで、そのプロセスを指定します。

［オペレーティングシステム］ラジオボタン

指定フォルダ・ドライブ以下への、OS からのアクセスログを除外します。

［全て］ラジオボタン

指定フォルダ・ドライブ以下への、全プロセスと OS からのアクセスログを除外します。

［ファイル・フォルダ］入力エリア *1

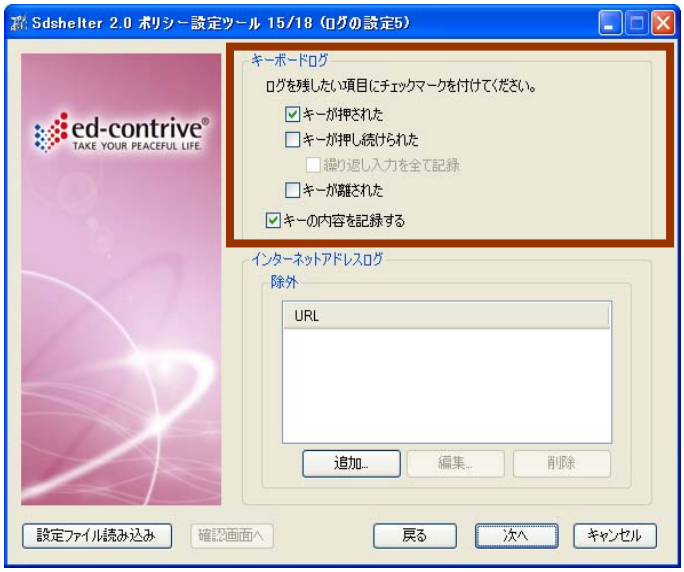
上記、プロセス等からのアクセスログを残したくない指定フォルダ・ドライブ以下のファイル・フォルダを直接入力か［参照］ボタンで指定します。

1 パス無し･絶対/相対パス、ファイル名はワイルドカード指定が可能です。例）C:¥ed¥.*

ログの設定４が完了したら、［次へ］をクリックします。

キーボードログの設定

ログ取得機能の設定で、キーボードログを有効にした場合に、設定が可能になります。
キーボードログとして残したい項目を選択してください。



［キーが押された］チェックボックス
［キーの内容を記録する］チェックボックスの設定により記録内容が異なります。
例）記録する：「E」が押されました ／ 記録しない：キーが押されました

［キーが押し続けられた］チェックボックス
［キーの内容を記録する］チェックボックスの設定により記録内容が異なります。
例）記録する：「E」が押し続けられています ／ 記録しない：キーが押し続けられています

［繰り返し入力を全て記録］チェックボックス
キーが押し続けられている間、繰り返し同一のログを記録します。上記の［キーが押し続けられた］でのログが連続で記録されます。
「繰り返し入力」とは、キーを押したままにした時に、連続的にそのキーが繰り返し入力されたように扱う OS の仕組みのことです。全てを記録することで、何が入力されたかを正確に記録することができますが、記録するログファイルのサイズは大きくなります。

［キーが離された］チェックボックス
［キーの内容を記録する］チェックボックスの設定により記録内容が異なります。
例）記録する：「E」が離されました ／ 記録しない：キーが離されました

［キーの内容を記録する］チェックボックス
選択の場合には、上記例）のように各操作での実際のキーの内容を記録します。
未選択の場合には、上記例）のように各操作での実際のキーの内容は記録しません。

インターネットアドレスログの設定

ログ取得機能の設定で、インターネットアドレスログを有効にした場合に、設定が可能になります。
ブラウザよりアクセスしたURLをインターネットアドレスログとして記録します。
対応ブラウザは Internet Explorer（プロトコルは http 又は https）のみです。
ログに残したくない URL は、除外リストに追加してください。

除外［追加］ボタン *1

［追加］ボタンをクリックすると、除外 URL の追加画面が表示されます。入力エリアに追加したい URL を直接入力してください。

除外［編集］ボタン *1

リストに表示されている除外 URL を選択後［編集］ボタンをクリックすると、除外 URL の編集画面が表示されます。入力エリアに表示されている選択除外 URL を直接編集してください。

除外［削除］ボタン

リストに表示されている除外 URL を選択後[削除]ボタンをクリックすると、選択除外 URL はリストから削除されます。

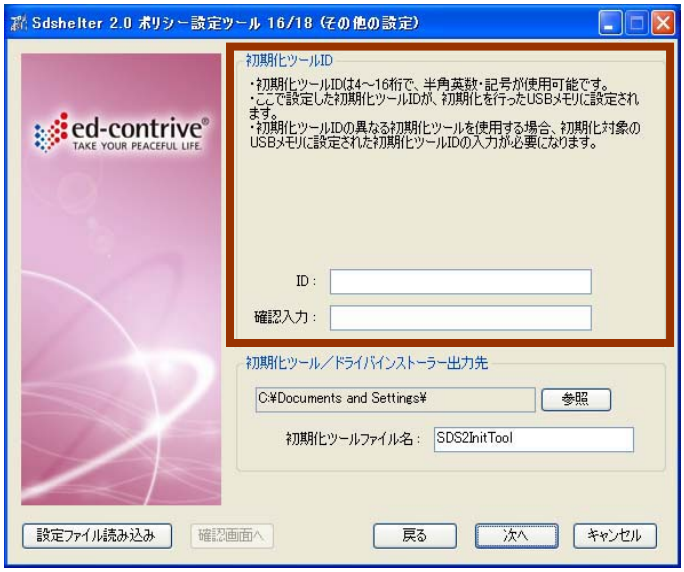
*1 例）

http://www.ed-contrive.co.jp/ ：左記 URL 以下の全ての URL を除外します。

http://www.ed-contrive.co.jp/index.html ：左記に一致する URL を除外します。

ログの設定５が完了したら、［次へ］をクリックします。

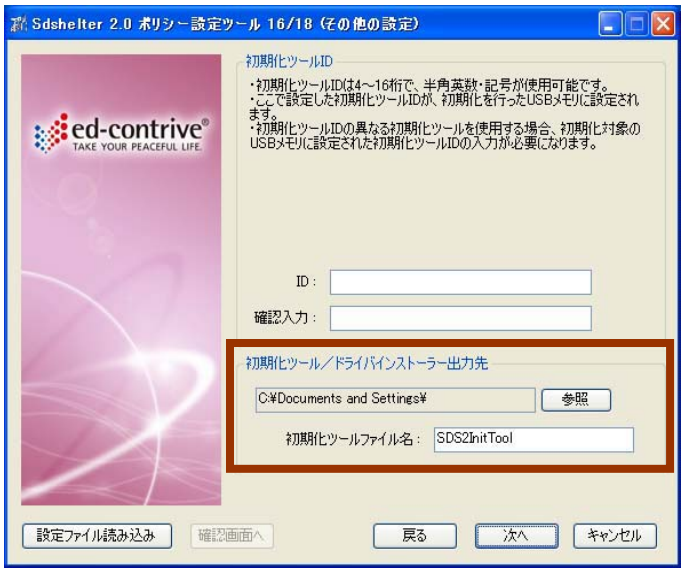
初期化ツール ID の設定



初期化ツール ID は、初期化ツール起動時に自動的にチェックされ、ID の異なる初期化ツールでの Sdshelter 2.0 の初期化を防止することにより、利用ユーザーによる USB メモリの勝手なポリシー変更を不可能にします。
また、Sdshelter 2.0 起動時には Sdshelter 2.0 側の初期化ツール ID とオフィス内ドライバ及びオフィス外ドライバ側の初期化ツール ID が一致した時のみパスワード認証画面を表示させる自動チェック機能にも使用します。

注意	＊ 新しい初期化ツールを作成して Sdshelter 2.0 の書き換えを行う場合には、Sdshelter 2.0 内に既に設定されている初期化ツール ID と同じ ID を入力してください。 ＊ 設定した初期化ツール ID の復元はできません。初期化ツール ID の取扱には十分注意し、お客様自身で管理してください。

初期化ツール／ドライバインストーラーの保存

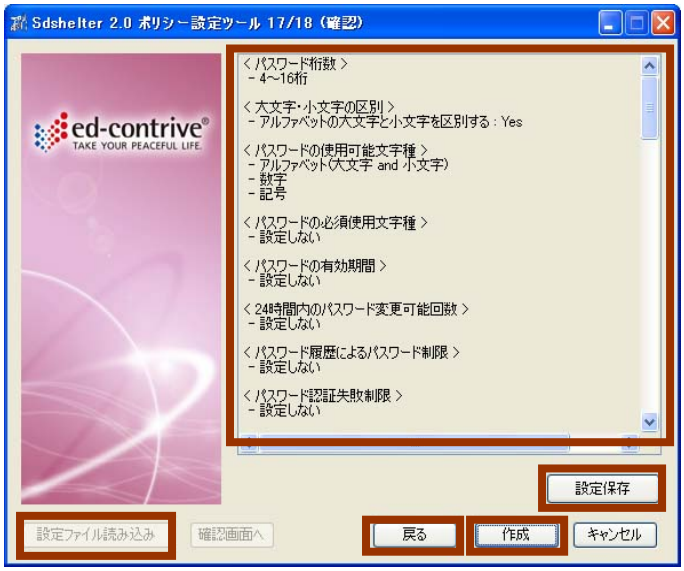


初期化ツールとオフィス内ドライバのインストーラーの出力先、及び初期化ツールのファイル名の設定を行います。
追加ファイルの設定で、管理用ドライブ内に、オフィス外ドライバのインストーラーを追加しない設定にした場合は、ここで設定した出力先にオフィス外ドライバのインストーラーも作成されます。

その他の設定が完了したら、［次へ］をクリックします。

設定内容の確認／設定の保存

設定した内容の確認画面が表示されますので、設定内容に問題がなければ［作成］ボタンをクリックし、初期化ツールとオフィス内ドライバのインストーラーを作成します。
追加ファイルの設定で、管理用ドライブ内に、オフィス外ドライバのインストーラーを追加しない設定にした場合は、オフィス外ドライバのインストーラーはここで作成されます。



設定内容を変更するには［戻る］ボタンをクリックします。

また、［設定保存］ボタンをクリックすることにより、設定した内容を保存しておくことが可能です。

設定した内容は［設定ファイル読み込み］ボタンから読み込むことが可能です。（［設定ファイル読み込み］ボタンは、本画面以前の設定操作時に実行することが可能です）

初期化ツールの使用

ポリシー設定ツールで作成した初期化ツールで、Sdshelter 2.0 を初期化し、ポリシー設定を適用します。同時に、必要なソフトウェア等（P. 5 参照）を Sdshelter 2.0 内に作成します。

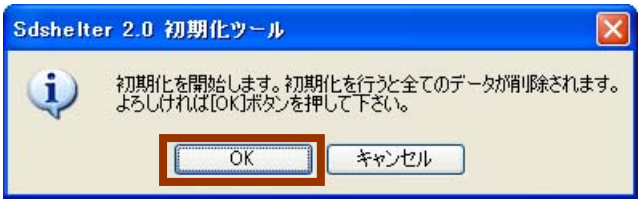
注意	＊ 初期化した場合には、USB メモリ内の既存データはログファイルも含め全て失われます。 ＊ 初期化ツールは管理者権限を持つアカウントでのみご使用いただけます。

1 初期化をする Sdshelter 2.0 を USB ポートに装着します。

＊ オフィス内ドライバ又はオフィス外ドライバがインストールされている PC では、パスワード設定もしくは、パスワード認証画面が自動的に表示されますので、必ずキャンセルしてください。

2 初期化ツール（ ）をダブルクリックします。

3 データ削除に関する確認画面が表示されますので、［OK］ボタンをクリックします。



4 初期化が開始されます。初期化中、Sdshelter 2.0 のドライブに関連のウィンドウが表示されることがありますが、初期化が完了するまでは Sdshelter 2.0 を抜かず、操作も行わないようにしてください。

5 完了画面が表示されたら、［OK］ボタンをクリックします。

使用可能期限の設定

使用可能期限の設定・再設定は、期限設定ツールをインストールしたアカウントで、期限を設定する Sdshelter 2.0 を接続して行います。

1 期限を設定する Sdshelter 2.0 を USB ポートに接続します。
＊ オフィス内ドライバ又はオフィス外ドライバがインストールされている PC では、パスワード設定もしくは、パスワード認証画面が自動的に表示されますので、必ずキャンセルしてください。

2 ［スタート］→［(すべての) プログラム］→［ED-CONTRIVE］→［Sdshelter 2.0］→［Sdshelter 2.0 期限設定ツール］を選択します。期限設定ツールが起動します。

注意	＊ 期限設定が有効になった Sdshelter 2.0 が接続されていないと、期限設定ツールは起動しません。

3 必要項目を入力します。現在のパスワード・現在の期限 ID はすでに設定されているときのみ入力が必要です。

メモ	＊ 期限 ID は管理者以外による期限の変更を防ぐために設定するものです。Sdshelter 2.0 に設定された期限 ID が分からないと期限の再設定はできません。 ＊ 期限 ID は、桁数・大文字と小文字の区別・使用可能文字種・使用しなければならない文字種についてパスワードと同様の制限がかかります。 ＊ ご利用の Sdshelter 2.0 が期限設定時に最大期間を設定している場合、期限設定操作を実行した日から最大期間を超えた日付の設定はできません。

4 必要項目を入力したら、［期限設定］ボタンをクリックします。設定が完了すると自動で PC から取り外し処理が行われます。

ロック解除・パスワード強制変更

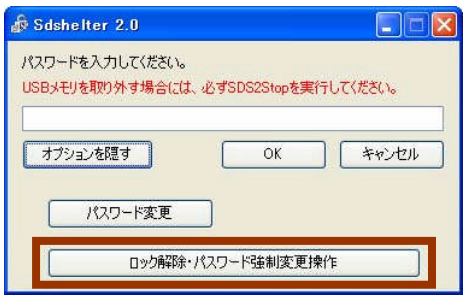
パスワード忘れ／ロック時の救済機能設定が有効な Sdshelter 2.0 に対して、パスワードの強制再設定、及びロック解除を行う手順について記します。

＜Sdshelter 2.0 での操作＞

1 パスワード認証画面の［オプションを表示］ボタンをクリックします。

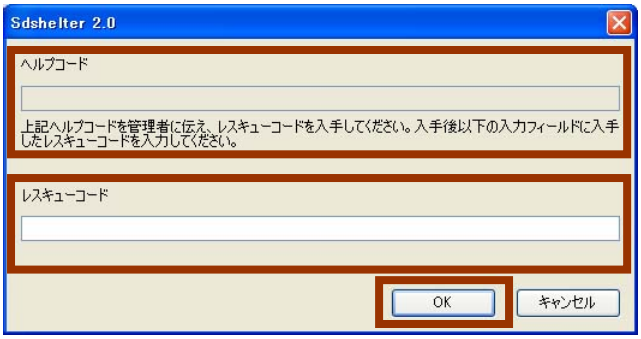
2 ［ロック解除・パスワード強制変更操作］ボタンをクリックします。

* パスワード忘れ／ロック時の救済機能設定が有効な時のみ［ロック解除・パスワード強制変更操作］ボタンが有効になります。

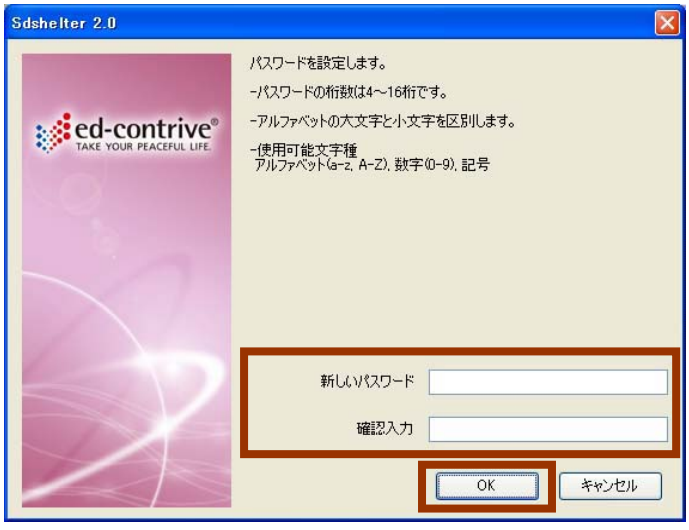


3 ヘルプコードが表示されますので、管理者に伝えてください。
（管理者：レスキューツールのご利用方法は次ページを参照ください）

4 管理者からレスキューコードを入手後、レスキューコードを入力し［OK］ボタンをクリックします。



5 正しいレスキューコードが入力された場合、パスワードの再設定画面が表示されますので新しいパスワードを入力して［OK］ボタンをクリックします。



＜レスキューツールでの操作＞

1 ［スタート］→［(すべての) プログラム］→［ED-CONTRIVE］→［Sdshelter 2.0］→［Sdshelter 2.0 レスキューツール］を選択します。レスキューツールが起動します。

2 レスキューID と Sdshelter 2.0 での操作で取得したヘルプコードを入力し、［生成］ボタンをクリックします。

3 レスキューコードが表示されますので、ユーザーに伝えてください。

ソフトウェア環境毎の主なドライバ機能の比較

下記、ソフトウェア環境下での 主なドライバ機能の比較	ﾊﾟｽﾜｰﾄﾞ認 証起動方法	コピー ガード制御	ﾈｯﾄﾜｰｸｱｸｾｽ と印刷
①ポリシー設定ツール	手動	無	可
②ポリシー設定ツール＋オフィス内ドライバ	自動・手動	無	可
③ポリシー設定ツール＋オフィス外ドライバ	自動・手動	有	設定による
④オフィス内ドライバ	自動・手動	無	可
⑤オフィス外ドライバ	自動・手動	有	設定による

＊ ①～③は、ポリシー設定ツールがインストールされているアカウント環境下です。
＊ レスキューツールや期限設定ツールのみのアカウント環境下では、Sdshelter 2.0 のパスワード認証画面は、起動できません。

下記、ソフトウェア環境下での 主なドライバ機能の比較	ｱｸｾｽ許可 ﾌﾟﾛｾｽ制限	ログの 閲覧	(ﾛｸﾞ取得有効) ログの記録
①ポリシー設定ツール	無	可	無
②ポリシー設定ツール＋オフィス内ドライバ	無	可	有
③ポリシー設定ツール＋オフィス外ドライバ	有	可	有
④オフィス内ドライバ	無	不可	有
⑤オフィス外ドライバ	有	不可	有

＊ ①～③は、ポリシー設定ツールがインストールされているアカウント環境下です。

＜［インストールレス機能（管理者権限時にオフィス外動作)］について＞

＊ 管理者権限を持つアカウントでのみご利用が可能です。
＊ Microsoft Windows 2000 ではご利用いただけません。
＊ 比較表{①ポリシー設定ツール}～{⑤オフィス外ドライバ}の各ソフトウェアがインストールされている環境下では、当機能が有効であってもインストールされている各ソフトウェア環境下として動作致します（各ソフトウェアの機能を優先します)。
ポリシー設定ツール・オフィス内ドライバ・オフィス外ドライバが、存在しないアカウント環境下で、当機能として動作致します。
＊ 比較表{⑤オフィス外ドライバ}と同等の機能を有します。但し、パスワード初期設定画面及びパスワード認証画面は、手動起動となります。また、Sdshelter 2.0 起動時における初期化ツール ID の自動チェック機能は、ありません。

＜その他＞

＊ オフィス内ドライバとオフィス外ドライバは、同一の PC にインストールを行うことはできません。
＊ SDS2Stop.exe の実行以外での Sdshelter 2.0 の取り外し（タスクトレイの安全な取り外しや、ツールを使用した取り外し等）は、行わないようにしてください。
必ず、SDS2Stop.exe を実行して Sdshelter 2.0 の取り外しを行ってください。

ソフトウェア使用許諾書

1　本ソフトウェアは、イーディーコントライブ株式会社の著作物です。したがって、本ソフトウェア及び本書の全部または一部を無断で複製、複写、転載、改変することは法律で禁じられています。

2　本ソフトウェア及び本書の内容については､改良のために予告なく変更することがあります。

3　本ソフトウェアの使用または使用できないことにより生じる損害、費用、派生的損害、間接的損害､付随的損害､特別損害､または利益の損失につき､いかなる責任も負いかねますので、予めご了承ください。

4　本ソフトウェアの著作権等の知的財産は､いかなる場合においてもお客様に移転されません。

5　本ソフトウェアのソースコードについては、いかなる場合においてもお客様に開示、使用許諾を致しません。また、ソースコードを解析するために本ソフトウェアを解析し、逆アセンブルや逆コンパイル、またはその他のリバースエンジニアリングをすることを禁止します。

6　書面による事前の承諾を得ずに本ソフトウェアをタイムシェアリング、リース、レンタル、販売、移転、サブライセンスすることを禁止します。

7　本製品に関し、日本国内でのみテクニカルサポート及びアフターサービス等を行っております。

8　本ソフトウェアは､「外国為替及び外国貿易法」の規定により戦略物資等輸送既製品に該当する場合があります。国外に持ち出す際には、日本国政府の輸出許可申請などの手続きが必要になる場合があります。

9　本ソフトウェアは医療機器や人命に直接間接的に関わるシステム、高い安全性が要求される設備や機器に組み込んでの使用は意図されておりません。これらのシステムや設備等に本ソフトウェアを使用され、本ソフトウェアの動作により人身事故、火災事故、社会的損害などが生じても、当社はいかなる責任も負いかねます。また、高い信頼性が要求される機器や電算機システムなどの用途に使用するときは､ご使用になるシステム等の安全設計や故障に対する適切な処置を万全に行ってください。

10 本ソフトウェアは､ツール毎に一時に一台のパソコンにおいてのみ使用することができます。

11 本ソフトウェアまたはその使用権を第三者に再使用許諾、譲渡、移転等の処分を行うことを禁止します。

12 本ソフトウェアに起因する債務不履行または不法行為に基づく損害賠償は、当社に故意または重大な過失があった場合を除き、本ソフトウェアの購入代金と同額を上限と致します。

13 当社は、お客様が上記のいずれかに違反された場合は、いつでも本ソフトウェアの使用を終了させることができるものとします。

Sdshelter 2.0 管理者ツール
取扱説明書
2009 年 11 月 第 4 版発行
発行：イーディーコントライブ株式会社